The Legal Hoops of Active Defense to CNA

By Richard P. Moore, Colonel, U.S. Air Force (Retired)

Editorial Abstract: *So called "Net Wars" between hackers from the U.S. and other countries pose challenging issues for those tasked with the defense of DOD networks. Of particular import is the decision to adopt a passive or an active defense. In this article, Colonel Moore discusses some of the legal requirements and restrictions imposed by an active defense against computer network attack.*

A CINC has been quoted as calling CNA (Computer Network Attack) "Computer – No Action." This is apparently in response to the widely perceived tendency of the legal experts within DoD to follow Nancy Reagan's motto of "Just Say No" when it comes to military operator proposals to conduct CNA. While this tendency may reflect recent history, it does not necessarily represent the final word of the legal community. In "AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS – SECOND EDITION," published by the Department of Defense Office of General Counsel[1], there is a detailed discussion of the legal issues surrounding "active defense," or launching a computer network attack on someone who is attacking DoD computer systems. That discussion lays out some very specific legal conditions that must be met for CNA to be legal under international law. The purpose of this paper is to examine the present situation between the United States and the People's Republic of China and outline a possible plan of action that would allow the US to use the situation as a test case for active defense. This would support one of the objectives listed in the referenced paper:

> "[I]t would be useful to create a process for determining when the response to a computer intrusion should shift from the customary law enforcement and counter-intelligence modes to a national defense mode. Such a process should include (1) a statement of general criteria to be applied; (2) identification of officials or agencies that will be involved in making the decision; and (3) procedures to be followed.[2]"

This process must be measured against world opinion:

> "As in all cases when a nation considers acting in self-defense, the nation considering such action will have to make its best judgment of how world opinion, or perhaps a body such as the International Court of Justice (ICJ) or the UNSC, is likely to apply the doctrine of self-defense to electronic attacks. As with many novel legal issues, we are likely to discover the answer only from experience.[3]"

> "Among the factors the NCA would probably consider would be the danger presented to U.S. national security from continuing attacks, whether immediate action is necessary, how much the sanctuary nation would be likely to object, and how the rest of the world community would be likely to respond.[4]"

FACTORS TO CONSIDER:

- Chinese self-defense
- Attribution
- "State sponsorship"
- Advising the offending nation
- Proportionality
- Crossing the territory of neutral states

Chinese Self-Defense

For the US to build a convincing case in the court of world opinion for "active defense," it must prove that it is acting in self-defense. This would be impossible to prove under current circumstances, since US hackers are invading Chinese web sites and defacing them. In fact, China could well build the case that they are acting in self-defense.

> "Chinese and U.S. hackers traded insults across the Internet as part of a threatened weeklong "Net War," breaking into dozens of corporate and government computers on both sides of the Pacific and replacing Web pages with political statements. On the U.S. side, there apparently have been no arrests of hackers targeting Chinese servers.[5]"

While there may be an inclination to applaud the activities of the US hackers for doing things that we would like to do if they were not illegal, the fact remains that the US is a nation of laws and the hacker activities are illegal. We can hardly, in clear conscience, pressure the Chinese to enforce their anti-hacking laws against those who are damaging our systems when we are not enforcing our own laws that prohibit those same activities.

Step one in the battle for world opinion should be, therefore, for the Department of Justice to mount a concerted effort to identify, arrest, and prosecute those US hackers who are attacking China. To the extent that we can find evidence of hackers from other countries participating in the attacks on China (Brazil is one nation that has been mentioned in the press),

we should exert pressure through diplomatic channels for those nations to find and prosecute their perpetrators. Only by taking publicly visible steps against our own hackers and their compatriots from other nations can we reasonably expect world opinion to sanction any further steps the US might take.

Attribution

> "[T]he international law of self-defense would not generally justify acts of 'active defense' across international boundaries unless the provocation could be attributed to an agent of the nation concerned.[6]"

> "U.S. officials said there was no evidence of Chinese government coordination of the hacker attacks against U.S. sites.[7]"

However, there is ample evidence that the hackers attacking US sites are Chinese.

> "In public discussion forums, Chinese hackers have described plans for a May 1 'Net War.' These hacker groups alternately call themselves the "Honker Union of China" and the "Red Guest Alliance." Most of the organization for the attacks apparently took place Monday in a single publicly accessible Internet chat room operated in China, where participants identified vulnerable computers. Within minutes after Web sites were so identified, vandals attacked them.[8]"

The present ROE for attacks on the DII allow system administrators to trace the attack back only one hop. Beyond that, they must call in law enforcement personnel to trace the attack. While this works well to protect the constitutional rights of American citizens, it is a hindrance to attribution of foreign attacks. SPACECOM and PACOM should request permission to track attacks on the DII back to their source as part of the normal ROE when it is strongly suspected that the attacks come from outside the US. A collateral effect of this change might be to make such traces inadmissible in court should the attacker turn out to be within the US, but it would make attribution much easier for those attacks which originate outside the country. Perhaps what is needed is a corollary to the rules against collecting information about "US persons" by the Intelligence Community. If intelligence collectors inadvertently collect such information, they must destroy it as soon as possible and report the collection to their superiors. Systems administrators for systems being attacked might be required to destroy all evidence that points to "US persons" and report their actions to their superiors. The procedures work well in the intelligence field and parallel procedures could, with proper training, also work in the Defensive Information Operations world.

"State Sponsorship"

Tracing an attack back to China does not necessarily mean that China sponsored the attack.

> "[S]tate sponsorship may be convincingly inferred from such factors as the state of relationships between the two countries, the prior involvement of the suspect state in computer network attacks, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks.[9]"

However, it is not necessary to prove state sponsorship if an attack has been traced back to an origin within that state's territory.

> "[T]he international law of self-defense would not generally justify acts of 'active defense' across international boundaries unless the provocation could be attributed to an agent of the nation concerned....or until the sanctuary nation has been put on notice and given the opportunity to put a stop to such private conduct in its territory and has failed to do so, or the circumstances demonstrate that such a request would be futile.[10]"

Advising the Offending Nation

> "Only if the requested nation is unwilling or unable to prevent recurrence does the doctrine of self-defense permit the injured nation to act in self-defense inside the territory of another nation. The U.S. cruise missile strikes against terrorists camps in Afghanistan on 20 August 1998 provides a close analogy in which the United States attacked camps belonging to a terrorist group located in the territory of a state which had clearly stated its intention to continue to provide a refuge for the terrorists. At some point, providing safe refuge for those who conduct attacks against another nation becomes complicity in those attacks. At a minimum, the offended nation is authorized to attack its tormenters, the terrorists. As complicity shades into the kinds of active support and direction that are commonly called 'state sponsorship,' military and leadership targets of the host state may themselves become lawful targets for acts of self-defense.[11]"

The US should thus file a formal complaint with China through diplomatic channels, insisting that China control its hackers as the US is doing. If China fails to do so, this would provide grounds for "active defense." However, the punishment must suit the crime, which brings us to proportionality.

Proportionality

> "A persistent foreign intruder who gains repeated unauthorized entry into a nation's computer systems by defeating a variety of security measures or who gains entry into a number of computer systems may demand a different response [from passive defense]. Such behavior may indicate both that there is a continuing danger and that coercive measures are necessary to stop the intruder's pattern of conduct. Similarly, there may be a right to use force in self-defense...when the intruder's conduct or the context of the activity clearly manifests a malicious intent.

> [T]he victim nation may be justified in launching a computer network attack in response, intended to disable the equipment being used by the intruder. Conducting a responsive computer network attack as a measure of self-defense against foreign computer network attacks would have the major advantage that it would minimize issues of proportionality, which would be more likely to arise if traditional military force were used.[12]"

It is hard to imagine a response that would be more proportional than "slicking the hard drive" of the attacker. This has the added bonus of being justifiable in terms of counter-intelligence in that it would also wipe out any intelligence information gained by the hacker during his penetration of US networks.

Crossing the Territory of Neutral States

This issue became a consideration during Operation EL DORADO CANYON, the strike on Libya in retaliation for the Libyan terrorist bombing of the La Belle Disco in Berlin that killed several Americans. France refused US aircraft staging from the UK permission to over fly France. However, this is not a consideration during CNA.

> "[E]ven during an international armed conflict international law does not require a neutral nation to restrict the use of its public communications networks by belligerents. Nations generally consent to the free use of their communications networks on a commercial or reciprocal basis. Accordingly, use of a nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty in the same way that would be a flight through its airspace by a military aircraft.[13]"

Summary of Recommended Actions

1 The Department of Justice should mount a concerted effort to identify, arrest, and prosecute those US hackers who are attacking China.

2 To the extent that we can find evidence of hackers from other countries participating in the attacks on China (Brazil is one nation that has been mentioned in the press), we should exert pressure through diplomatic channels for those nations to find and prosecute their perpetrators.

3 SPACECOM and PACOM should request permission to track attacks on the DII back to their source as part of the normal ROE when it is strongly suspected that the attacks come from outside the US.

4 Develop a corollary to the rules against collecting information about "US persons" by the Intelligence Community.

5 The US should file a formal complaint with China through diplomatic channels, insisting that China control its hackers as the US is doing.

6 Publicize the first, second, and fifth bullets above through press releases to prepare world opinion for a retaliatory "active defense" CNA strike against China.

7 Prepare press releases to counter any allegation that the US illegally crossed neutral territory in effecting its CNA.

8 If Chinese hackers continue attacking US systems long enough for all of the above to be completed, conduct an "active defense" CNA operation against them.

End Notes

[1] Johnson, Phillip A. (Colonel USAF, Retired), "AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS – SECOND EDITION", NOVEMBER 1999, Department of Defense Office of General Counsel, with contributions from the General Counsels of the Army, Navy, Air Force, the National Security Agency and the Defense Information Systems Agency, as well as the Judge Advocates General of the military services and the Legal Counsel of the Chairman of the Joint Chiefs of Staff, thus representing a consensus of the military legal community.

[2] Ibid, page 22.

[3] Ibid, page 18.

[4] Ibid, page 21.

[5] Bridis, Ted, "U.S., Chinese Hackers Break Into One Another's Sites, Trade Insults," Staff Reporter of The Wall Street Journal, May 1, 2001

[6] Johnson, page 21.

[7] Bridis

[8] Ibid

[9] Johnson, page 20.

[10] Ibid, page 21.

[11] Ibid, page 20.

[12] Ibid, page 18.

[13] Ibid, page 21.

Col Richard P. Moore, (USAF, retire Principal Analyst with the General Resear Corporation International (GRCI), is developer of the Joint IO Planning Process.

Mr. Moore's U.S. Air Force career included tours in Turkey, Italy, Portugal, and Panama. He was the operations officer of three Electronic Security Command units, the Consolidated Cryptologic Program Eleme Monitor at the Air Staff and, in his last active d assignment, was the Chief of the US So Command Joint Intelligence Center.

Since retiring from the Air Force, Mr. Moore has held several program management, analytical, and software development positions in the defense industry. He currently serves as a GRCI principal consultant to the Operations Directorate, Joint Information Operations Center.